PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/32

A1

(11) International Publication Number: **WO 00/39958**

(43) International Publication Date: 6 July 2000 (06.07.00)

(21) International Application Number: PCT/FI99/01036

(22) International Filing Date: 15 December 1999 (15.12.99)

(30) Priority Data:
982728 16 December 1998 (16.12.98) FI

(71) Applicant *(for all designated States except US)*: SONERA OYJ [FI/FI]; Teollisuuskatu 15, FIN–00510 Helsinki (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: VATANEN, Harri [FI/GB]; 40 Alma Road, Windsor, Berkshire SL4 3HJ (GB).

(74) Agent: PAPULA REIN LAHTELA OY; P.O. Box 981 (Fredrikinkatu 61 A), FIN–00101 Helsinki (FI).

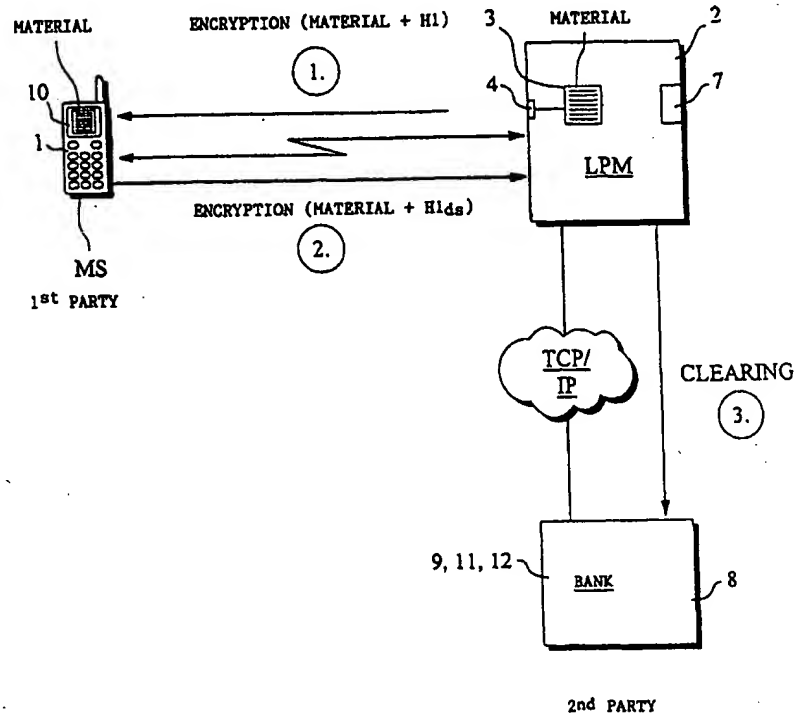
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
In English translation (filed in Finnish).

(54) Title: METHOD AND SYSTEM FOR IMPLEMENTING A DIGITAL SIGNATURE

(57) Abstract

Method for digitally signing an electronic form in a secure manner by means of a mobile station. In the method, the material to be signed, which comprises a form, its identifier, shared information, and/or essential information added to it, is transferred to the mobile station, a first hash code (H1) is computed from the material to be signed, the hash code is added to the material for transfer into the mobile station, the material transferred into the mobile station is signed digitally by means of the mobile station and the authenticity of the signed and transferred material is verified by comparing the signed hash code with the hash code computed from the material before the signature. Thanks to the invention, a mobile station can be safely used for digital signature in various applications.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND SYSTEM FOR IMPLEMENTING A DIGITAL SIGNATURE

The present invention relates to telecommunication systems and to a technique for signing and encrypting digital information. In particular, the invention relates to a system which makes it possible to sign an electronic form or other electronic information and to verify the authenticity of the signature and the signatory.

BACKGROUND OF THE INVENTION

In prior art, the use of a digital mobile station, e.g. a mobile station in the GSM system (Global System for Mobile communications, GSM), for commercial transactions, such as paying a bill or making a payment by electronic means, is known. Patent application US 5,221,838 presents a device which can be used for making a payment. The specification describes an electronic payment system in which a terminal device capable of wired and/or wireless data transfer is used as a payment terminal. The terminal device according to the specification comprises a card reader, a keypad, a bar code reader for the input of information and a display unit for presenting the payment information.

Patent specification WO 94/11849 discloses a method for the utilization of telecommunication services and execution of payment transactions via a mobile telephone system. The specification describes a system comprising a terminal device which communicates over a telecommunication system with a service provider's mainframe computer containing the service provider's payment system. The terminal device used in a mobile telephone network, i.e. the mobile station, can be provided with a subscriber identity module comprising subscriber information for the identification of the subscriber and for the encryption of telecommuni-

cation. The information can be read into the terminal device so that it can be used in mobile stations. The specification mentions the GSM system as an example, in which a SIM card (Subscriber Identity Module, SIM) is used as a subscriber identification unit.

In the system according to WO 94/11849, the mobile station communicates with a base station comprised in the mobile telephone network. According to the specification, a connection is further established with the payment system, and the amount to be paid as well as the data required for the identification of the subscriber are transmitted into the payment system. In the bank service described in the specification, the client places a service card given by the bank and containing a SIM unit into a terminal device used in the GSM network. In telephone based bank service, the terminal device may be a GSM mobile station consistent with the standard. Using the method described in the specification, a wireless telecommunication connection can be used for making payments and/or paying bills or implementing other bank or cash services.

The problem with the above-mentioned solutions is that they do not involve any consideration of reliability of the payment from the payer's and the payee's point of view. When a mobile station is used for making a payment, it is important that both the payer and the payee can trust the system. The payer must know exactly what he is paying for, how much he is paying, to whom he is paying, how he is paying etc. The payee must also know exactly who is paying for what and how much etc.

As is well known, transmitting information in electronic form from one place to another is easy. However, it is more difficult to make sure that the information transmitted remains unchanged during the transmission and that e.g. the information presented

on the display of a mobile telephone is transmitted in exactly the same form and unchanged to the receiver.

A previously known practice is to use a hash code, which is a data field formed and computed from the information to be transmitted. The hash code is generally computed using an algorithm which is a one-way function, in other words, the hash code can not be deciphered so as to reveal the information from which it has been generated. An algorithm that may be used for this purpose is SHA-1 (Secure Hash Algorithm).

A digital signature, which is considered as a general requirement in electronic payment, is used to verify the integrity of the material transmitted and the origin of the sender. A digital signature is generated by encrypting a hash code computed from the material to be transmitted, using the sender's secret key. As nobody else knows the sender's secret key, the receiver decrypting the encrypted material can be assured that the material is unchanged and generated by the sender. An example of an algorithm used in digital signatures is the RSA encryption algorithm, which is an encryption system based on a private key and a public key and which is also used for the encryption of messages.

OBJECT OF THE INVENTION

The object of the present invention is to eliminate the problems referred to above. A specific object of the invention is to disclose a new type of method and system for the signing of a form or corresponding information by means of a mobile station. In this context, `form' may refer to many types of message, dispatch or information structure with various contents. The form may consist of object type or software object type information which can be processed in electronic form.

A further object of the invention is to disclose a simple method for implementing commercial transactions, such as paying a bill and transacting business with a bank, using a mobile station, a method that is easy to implement with present technology.

SUBJECT OF THE INVENTION

The invention concerns a method for signing an electronic form as defined above with a digital signature in a secure manner using a mobile station or some other equivalent and comparable device. In the method, the material to be signed, which may comprise at least the form, its identifier, shared data, and/or essential information added to the form, is transferred into the mobile station. The material to be signed can also be generated from an identifier of the form and essential information associated with the form; for instance, in the case of a bank transfer form, the material to be signed may be generated from the identifier of the bank transfer form and the data in the essential fields in it, such as the payer, payee and amount fields.

According to the invention, from the material to be signed, a first hash code is computed, preferably before the material is transferred into the mobile station. The hash code is added to the material, to be transferred with it, thus allowing the hash code to be used as an aid in verification. After the material has been transferred into the mobile station, it is signed in the mobile station and, further according to the invention, the authenticity and conformity of the signed and transferred material are verified by comparing the signed hash code with the hash code computed from the material before signature. The signature can also be accomplished by signing both the essential information and the hash code, in which case it will even ensure that the material signed via the

mobile station corresponds to the material transferred for signature.

In the case of certain types of application, such as payment applications, the material transferred into the mobile station can also be transferred to a second party, e.g. a bank, which can compute a hash code from the material received. The material signed in the mobile station can further be encrypted and the encrypted and signed material can be transferred from the mobile station to the second party as well. The second party decrypts the encrypted information, verifies the signature, computes a second hash code from the material received from the mobile station and compares it with the first hash code computed from the original material. If the second party accepts the digital signature and if the first and second hash codes correspond to each other, then the bank will accept the signature made via the mobile station. After the bank has accepted the signature, it can put a time stamp in the signed and encrypted material and file the transaction of signature of the material.

The case described above is a procedure in which a client of a bank signs a form received from the bank. The client or mobile station user may communicate locally with an automated payment machine or equivalent, in which case the payment machine transmits to the client a form for payment and approval. In this case, the client exchanges messages with the payment machine locally and the payment machine transmits the digital signature data further. However, the payment machine can infer from the communication it is transmitting that the client has accepted the service and payment form offered to it. The machine can serve the client locally in a manner desired and paid for by the client, without necessarily waiting for the bank's approval of it. In practice, the situation corresponds to the normal practice where e.g. a customer at a

shop's cash machine pays for products or services with a cash card and the shop provides them to the customer without verifying the authenticity of the payment by contacting the bank.

The material can also be encrypted before being transferred into the mobile station, in which case the material has to be decrypted in the mobile station before signature. This expedient can be used to ensure that only the desired mobile station will receive the material to be transferred and to guarantee the security of the information.

The form can be generated using a pre-agreed form overlay, message structure or any other information structure, provided with an identifier, in which pre-agreed essential information is filled in before the form is transferred into the mobile station. The hash code can be computed using e.g. a hash function. For the signature and/or encryption of the message and/or form, a public and private key method can be used.

In a preferred embodiment of the invention, the material and/or part of it is presented in the mobile station prior to the signing of the material. For example, the payee, payer and reference information and the amount payable may be presented. It is also possible to require that the mobile station be started in signature mode before the transfer of the material into it. In practice, this may mean that the user of the mobile station has to enter another predetermined PIN code with which the mobile station has been configured to start in a predetermined signature mode. Thus, it is possible to use a kind of local authentication.

The invention also concerns a system for digitally signing an electronic form in a secure manner using a mobile station. The system preferably comprises a payment machine and, connected to it, means

for generating the material to be signed and transferring it into the mobile station, said material being as defined above. In this context, `payment machine' may refer to any local or locally operated automated machine capable of communicating over a telecommunication network with a service provider, such as a bank, shop or equivalent.

The payment machine may also be implemented locally in a computer which communicates with the service provider e.g. over the Internet, the service provider providing products and services via the Internet. In this case, the material to be signed is transferred for signature from the computer into the mobile station using a local connection or directly from the service provider's own server without using a local computer and local connection.

According to the invention, the payment machine comprises means for computing a first hash code from the material to be signed. Moreover, the mobile station comprises signing means for the signing of the material transferred into it. The signing means may comprise a memory in which the algorithms and keys required for the signature and encryption are stored, and a processor which is connected to the memory and which processes the material, implementing the signature and possibly encryption. In addition, the payment machine comprises means for verifying the authenticity of the signed material transferred by comparing a hash code signed in the mobile station with a hash code computed from the material before signature.

The system may also comprise a sever which is connected to the payment machine and/or to the mobile station and which is controlled by a second party, such as a bank or credit card company. Such a server may thus be maintained e.g. by a bank and it can be used in the implementation of bank transactions. The server may also comprise means for the verification of

the authenticity of a digital signature made by a mobile station and encrypting and decrypting means for the encryption and/or decryption of material transferred between the server and the payment machine and/or mobile station.

The server may also comprise means for stamping the material with a time stamp and means for filing the transaction of signature of the material after the signature has been authenticated. These can be implemented in a manner known in itself to the skilled person, so they will not be described here in detail.

As compared with prior art, the present invention provides the advantage of facilitating the implementation of payment applications, verification transactions and the like. Thanks to the invention, a mobile station can be reliably used for making a digital signature, and a digital signature can be incorporated in many different applications.

LIST OF ILLUSTRATIONS

In the following, the invention will be described by the aid of a few examples of its preferred embodiments with reference to the attached drawing, wherein

Fig. 1 presents a preferred system according to the present invention;

Fig. 2 presents another preferred system according to the present invention;

Fig. 3 presents a preferred embodiment of the present invention in the form of a flow diagram; and

Fig. 4 is a diagrammatic representation of a preferred example of the generation of the material to be signed in conjunction with the present invention.

The system presented in Fig. 1 comprises a local payment machine (LPM) 2 and, connected to it, means for generating the material to be signed, comprising a form, its identifier, shared data and/or es-

sential information associated with it. In addition, means 4 connected to it for transferring the material to a mobile station. Correspondingly, the mobile station comprises means 1 used by the mobile station (MS) to communicate with the payment machine. In an embodiment, means 1 and 4 are implemented using the Bluetooth technology. A more detailed description of the Bluetooth technology will be found e.g. on WWW page www.bluetooth.com. Other known link access protocols, such as the infrared interface, may also be used.

The system presented in Fig. 1 further comprises a server 8 which is connected via a TCP/IP link to the payment machine 2 and which in this example is managed by a bank. The server further comprises means 9 for verifying the authenticity of the signature - in practice, these means are used to decrypt the encrypted messages received and to compare the digital signatures contained in them with the user information received. Moreover, the server comprises means 11 and 12 for stamping the signed material with a time stamp and filing the signing transaction after the signature has be authenticated. Corresponding verification means may also be comprised in the payment machine, and in this example they are indicated by the number 7. Means 7, 11 and 12 may also have a feature for fetching the required public keys from universal key management servers e.g. via a TCP/IP network.

In the example presented in Fig. 1, the encrypted material, comprising an invoice form and a hash code H1 computed from it, is transferred from the payment machine 2 into the mobile station MS, step 1. In the mobile station, the material, i.e. the invoice form and the payee, payer, amount and reference number of the payment, are presented on the display (10) of the mobile telephone, allowing the user of the mobile station to check what he/she is signing. Using the mobile station MS, the user then signs the material and

the hash code H1 computed from it. The material with the digitally signed hash code $H1_{ds}$ added to it is transferred into the payment machine 2, step 2. The messages transmitted between the payment machine 2 the mobile station MS can be encrypted using public and private keys of the mobile station user and the payment machine. After the authenticity of the signature has been verified in the payment machine 2, a clearing message is sent from the payment machine to the bank, step 3. Clearing is a known practice generally used in banking, so it will not be described here in detail.

Reference is now made to Fig. 2, which presents a system corresponding to Fig. 1, but in this case the system is used in a somewhat different manner. First, the material generated in the payment machine, e.g. a form, is transferred to the bank, step 1. Next, in the payment machine, a hash code H1 is computed from the material and transferred to the mobile station for signature, step 2. The transfer can be implemented using a local link, e.g. a Bluetooth connection. In the mobile station, the message received is signed digitally, whereupon the signed and possibly encrypted material is sent to the bank, step 3. In the bank, the hash code H1 computed from the material received from the payment machine is compared with the digitally signed hash code $H1_{ds}$ received from the mobile station, and if the two hash codes match, then the signing transaction is approved. After this, using a server, a time stamp is added and the signing transaction thus obtained is filed. The bank may also be some other corresponding service provider, such as a credit card company, in which case, in addition to the above description, a confirmation of authenticity of the signature is sent to the bank, payment machine or other service provider. In this case, the credit card company, after confirming the signature, takes responsibility for the transaction.

Referring to Fig. 3, a preferred embodiment of the invention will be described. First, the material to be signed by means of a mobile station is generated, block 31. From the material, a first hash code H1 is computed, block 32. Next, block 45, a check is performed to establish whether the material has to be encrypted before transmission. If the material has to be encrypted, then the procedure goes on to block 46 and the material is encrypted using the mobile station user's public key. After the encryption, the procedure goes on to block 33. If the material need not be encrypted, then action proceeds directly to block 33, where the material is transferred to the mobile station. Next, the procedure goes on to block 34, and the user checks the material or the essential information in it, presented on the display of the mobile station, in other words, the user checks whether e.g. the payee and the payment in an invoice are correct. If the payer agrees, in block 35, then action proceeds to block 37 and the material is signed. If the payer does not agree in block 35, then the procedure goes on to block 36, where a reject message is sent to the sender of the material, e.g. a payment machine, and the process is stopped. From block 37, action proceeds to block 38, where a data aggregate is generated from the digital signature and hash code and possibly from the material received, comprising e.g. the essential information contained in the form, block 38. After that, the data aggregate is transferred to the payment machine, block 39, from where the process goes on to block 40, where the hash code computed from the transferred material is compared with the signed hash code. If the hash codes match, block 41, then the signature is accepted and the further actions defined are carried out.

If in block 40 the hash codes did not match, then the procedure can be repeated. At this point it

is possible to use a counter to check that the material will not be sent more times than previously agreed. From block 40, the procedure goes on to block 43, where the value of a counter k = k + 1 is incremented by one, whereupon action proceeds to block 44, where the value of the counter is checked, this value indicating the number of times the material has been transferred to the mobile station. If the value exceeds a pre-agreed limit, then the procedure goes on to block 42 and a reject message is sent to the mobile station. If the value of the counter is smaller than the pre-agreed limit, then the procedure returns to block 31 and the process is repeated.

Fig. 4 illustrates a preferred way of digitally generating and signing the form or material. The material to be transferred to the mobile station comprises a form identifier, block 51, all the forms used having unique identifiers. Associated with the form identifier is a form template, block 52; based on these, the applications, the client and the provider of the application know exactly what type of form is being used in each case. When the material is being generated, the form identifier and the form template are chained sequentially as illustrated in Fig. 4, whereupon a first hash code is computed from them, block 54.

In many cases, form data is added to the form, block 53, even before the form is transferred to the mobile station for signature. In this case, the form identifier and the form data are concatenated in the order indicated in Fig. 4 and the bit sequence obtained from them is further concatenated with sixteen random bytes, block 55. The first hash code from block 54 is combined with these data.

At this point, the material is ready to be transferred to the mobile station, whereupon a second hash code is computed from it, block 56. In practice,

the second hash code is computed in the mobile station and added to the message to be signed, block 57. Likewise, user data, which the mobile station user may have complemented with personal information as needed, has been added to the message to be signed. To this message to be signed are preferably also added the 16 random bytes from block 55, thus making it possible to verify the authenticity of the signed message generated by the party transferring the material and the mobile station user. After the random bytes, the user data and the second hash code have been set in sequence, the message is signed digitally in the user's mobile station. After this, the message can be transmitted further to a second party, to a payment machine or other original source of the material.

In summary, let it be further stated that the invention purports to implement a method and system in which a user, a service provider and a bank, which are mentioned as an example, are able to verify the authenticity of a digital signature. The objective is to enable the material to be signed to be bound to some user data, format and a digital signature made by the user. In other words, it must be possible to bind the signature to a certain kind of chain, which in practice corresponds to the currently used chain in which the user confirms a purchase by his/her own manual signature. Similarly, the object of the method is to identify the signatory in a reliable manner as required and intended by the legislator.

The invention is not restricted to the examples described above, but many variations are possible within the limits of the sphere of protection defined by the claims.

CLAIMS

1. Method for digitally signing an electronic form in a secure manner by means of a mobile station, said method comprising the steps of

transferring the material to be signed, which comprises the form, its identifier, shared information, and/or essential information added to it, to the mobile station, characterized in that

a first hash code (H1) is computed from the material to be signed;

the hash code is added to the material, to be transferred to the mobile station;

the material transferred to the mobile station is signed digitally by means of the mobile station; and

the authenticity of the signed and transferred material is verified by comparing the signed hash code with the hash code computed from the material before signature.

2. Method as defined in claim 1, characterized in that

the material transferred to the mobile station for signature is transferred to a second party; and

the signed material is transferred to the second party, whereupon the second party verifies the authenticity of the signature.

3. Method as defined in claim 1 or 2, characterized in that

the material is encrypted before being transferred between the mobile station and the second party; and

the encrypted material is decrypted before any treatment of the material, such as signature and verification of authenticity.

4. Method as defined in any one of the preceding claims 1 - 3, characterized in that

the form is generated using a pre-agreed form template provided with an identifier, the essential information being filled in in the form template before it is transferred to the mobile station.

5. Method as defined in any one of the preceding claims 1 - 4, characterized in that the hash code is generated using a hash function.

6. Method as defined in any one of the preceding claims 1 - 5, characterized in that the signature and/or encryption of the message is implemented using a public and private key method.

7. Method as defined in any one of the preceding claims 1 - 6, characterized in that the material and/or part of it is presented in the mobile station before the material is signed.

8. Method as defined in any one of the preceding claims 1 - 7, characterized in that the mobile station is started in signature mode before the transfer of the material into the mobile station.

9. Method as defined in any one of the preceding claims 1 - 8, characterized in that the material is stamped with a time stamp; and

the transaction of signature of the material is filed after the signature has been authenticated.

10. System for digitally signing an electronic form in a secure manner by means of a mobile station (MS), said system comprising

a payment machine (2);

means (3) connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it; and

means (4) connected to the payment machine for the transfer of the material into the mobile station (MS), c h a r a c t e r i z e d in that

the payment machine comprises means (5) for computing a first hash code (H1) from the material to be signed;

the mobile station comprises signing means (6) for the signing of the material transferred into it; and

the payment machine comprises means (7) for verifying the authenticity of the signed and transferred material by comparing s signed hash code ($H1_{ds}$) with the hash code (H1) computed from the material before signature.

11. System as defined in claim 10, c h a r a c t e r i z e d in that the system comprises

a server (8) connected to the payment machine (2) and the mobile station (MS) and controlled by a third party; and

the mobile station comprises means for encrypting the signed material.

12. System as defined in claim 10 or 11, c h a r a c t e r i z e d in that the server (8) comprises

means (9) for the verification of authenticity of the digital signature.

13. System as defined in any one of the preceding claims 10 - 12, c h a r a c t e r i z e d in that the mobile station comprises

means (10) for presenting the material and/or part of it in the mobile station before the signing of the material.

14. System as defined in any one of the preceding claims 10 - 13, c h a r a c t e r i z e d in that the server (8) comprises

means (11) for stamping the material with a time stamp; and

means (12) for filing the transaction of signing of the material after the signature has been authenticated.

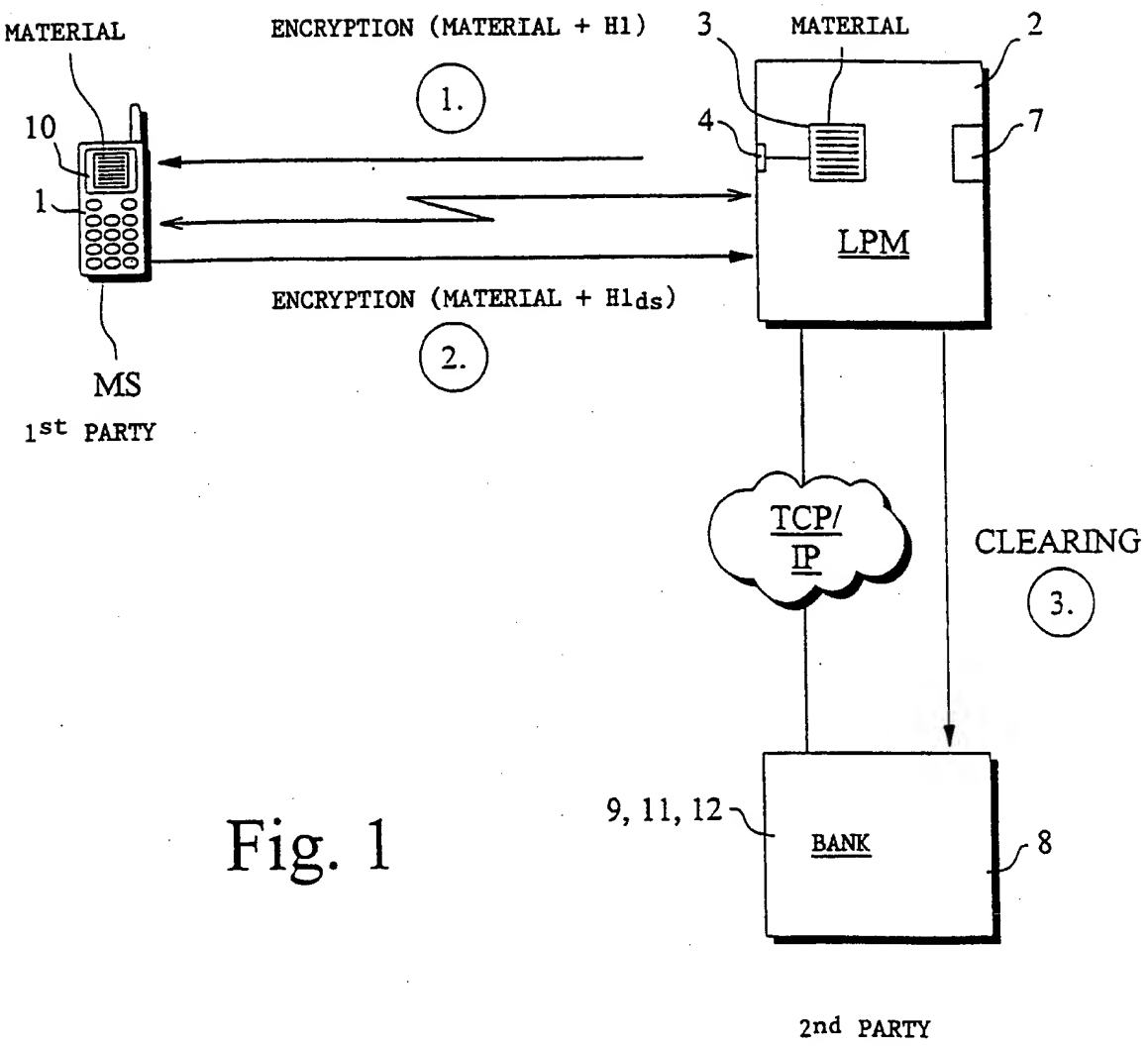

MATERIAL
ENCRYPTION (MATERIAL + H1)
1.
3
MATERIAL
2
10
4
7
1
LPM
ENCRYPTION (MATERIAL + H1ds)
2.
MS
1st PARTY
TCP/
IP
CLEARING
3.
9, 11, 12
BANK
8
2nd PARTY

Fig. 1

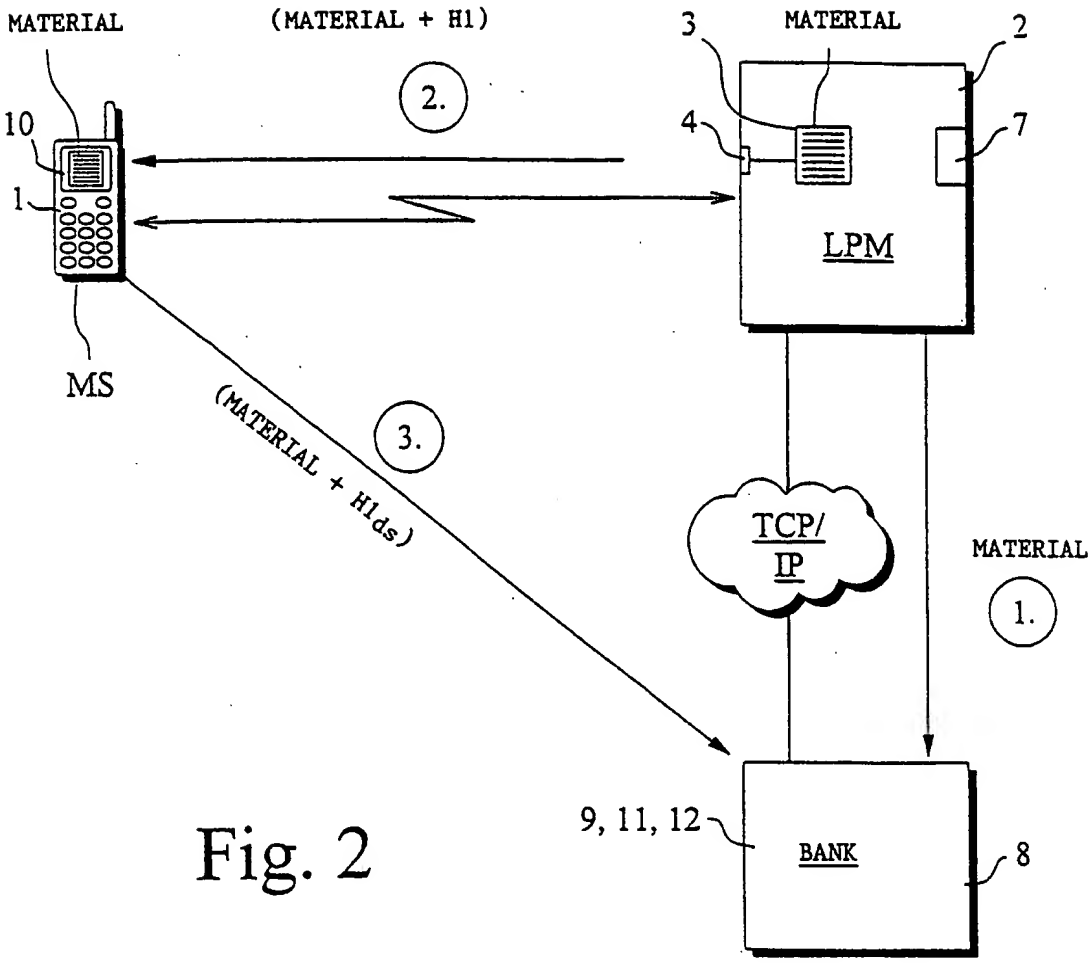

MATERIAL
(MATERIAL + H1)
2.
3
MATERIAL
2
10
4
7
1
LPM
MS
(MATERIAL + H1ds)
3.
TCP/
IP
MATERIAL
1.
9, 11, 12
BANK
8

Fig. 2

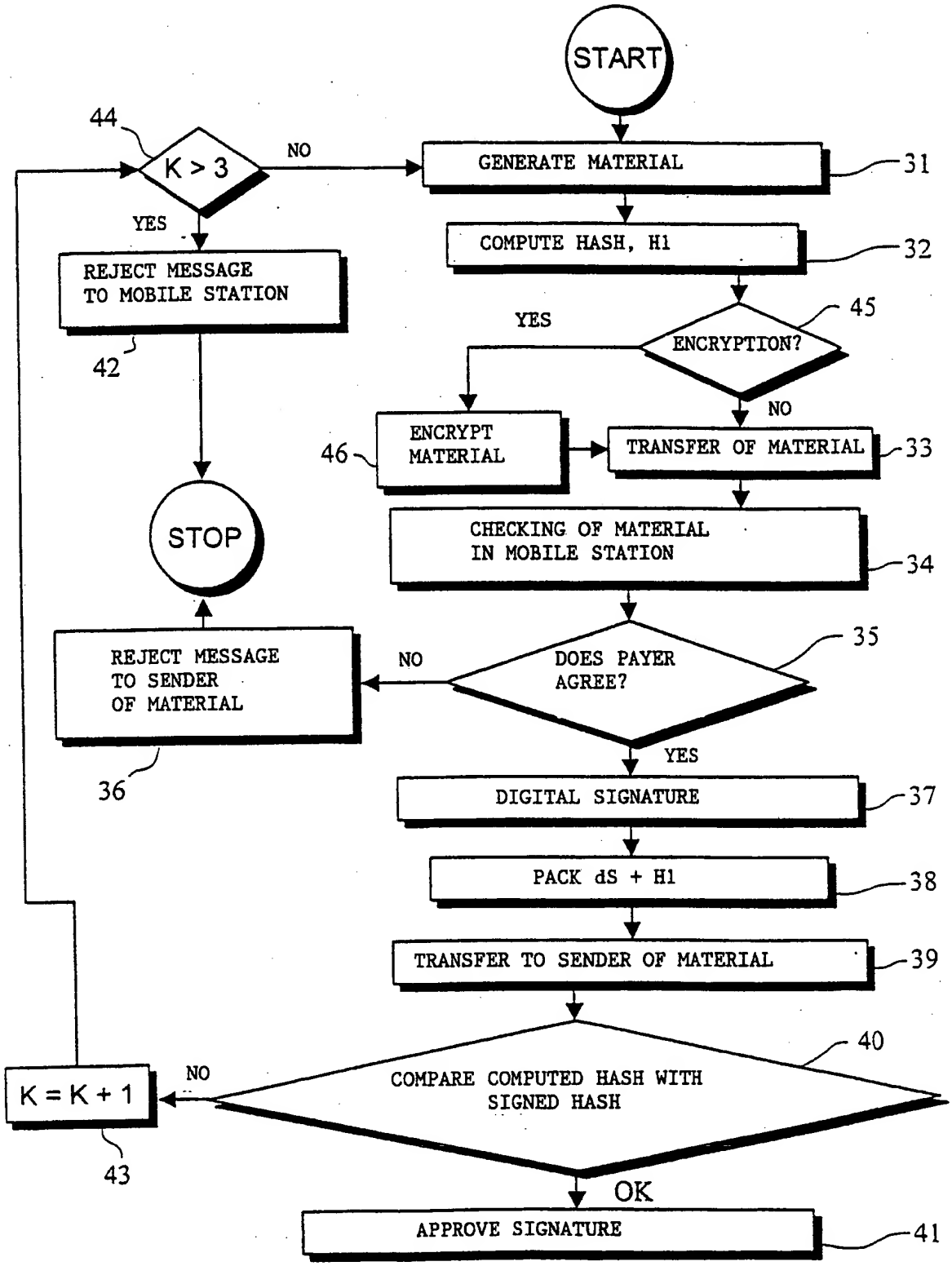

START
GENERATE MATERIAL
31
COMPUTE HASH, H1
32
ENCRYPTION?
45
YES
NO
ENCRYPT MATERIAL
46
TRANSFER OF MATERIAL
33
CHECKING OF MATERIAL IN MOBILE STATION
34
DOES PAYER AGREE?
35
NO
YES
REJECT MESSAGE TO SENDER OF MATERIAL
36
DIGITAL SIGNATURE
37
PACK dS + H1
38
TRANSFER TO SENDER OF MATERIAL
39
COMPARE COMPUTED HASH WITH SIGNED HASH
40
NO
OK
APPROVE SIGNATURE
41
K = K + 1
43
K > 3
44
YES
NO
REJECT MESSAGE TO MOBILE STATION
42
STOP

Fig. 3

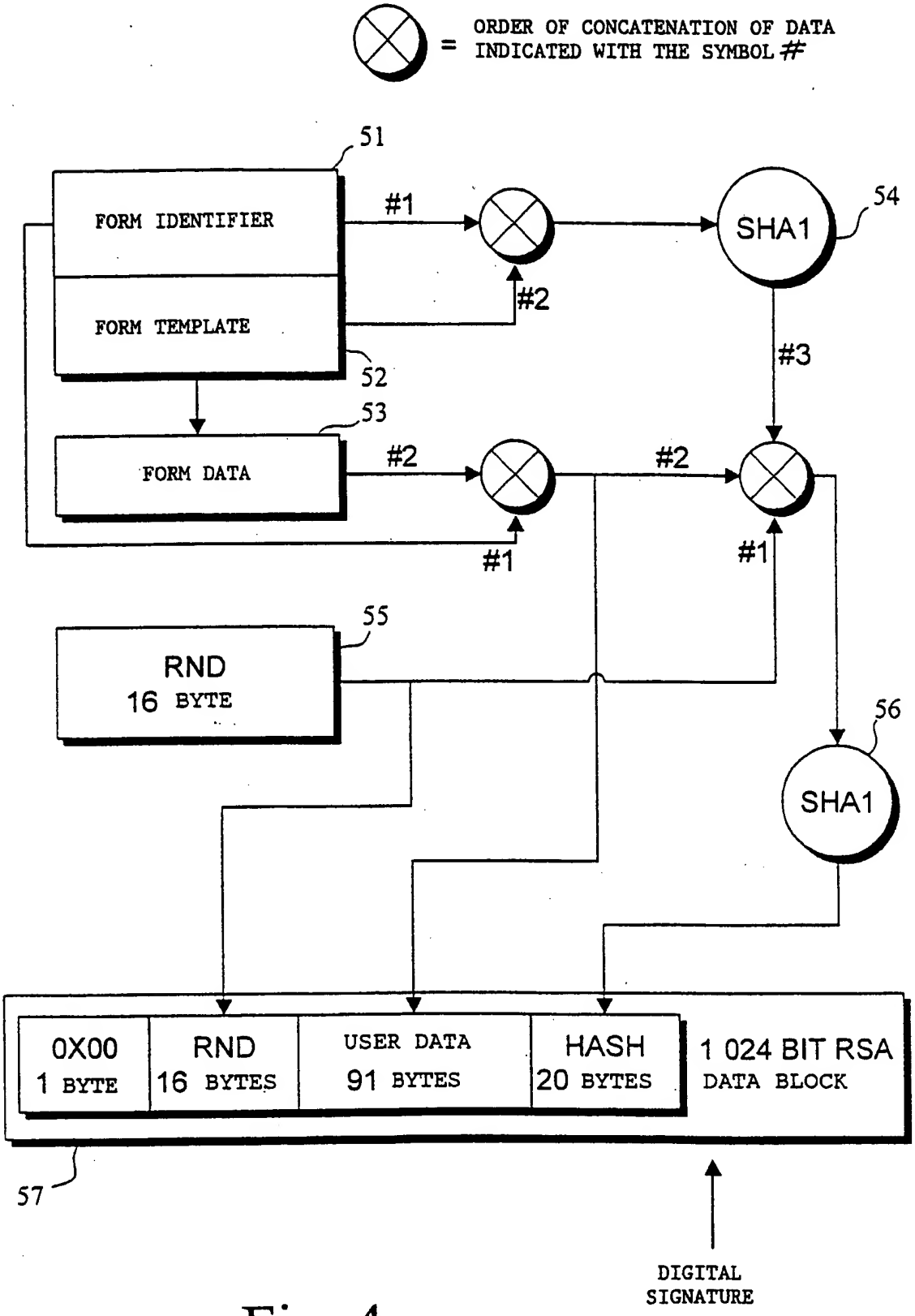

= ORDER OF CONCATENATION OF DATA INDICATED WITH THE SYMBOL #
51
FORM IDENTIFIER
FORM TEMPLATE
52
#1
#2
SHA1
54
#3
53
FORM DATA
#2
#2
#1
#1
55
RND
16 BYTE
56
SHA1
0X00
1 BYTE
RND
16 BYTES
USER DATA
91 BYTES
HASH
20 BYTES
1 024 BIT RSA
DATA BLOCK
57
DIGITAL
SIGNATURE

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/01036

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0689316 A2 (AT & T CORP.), 27 December 1995 (27.12.95), figure 1, abstract --	1-14
X	William Stallings, "Data and Computer Communications", 1997, Prentice-Hall International, Inc., (London), page 638 - page 649, figure 18.11(b) --	1
X	US 5018196 A (K. TAKARAGI ET AL.), 21 May 1991 (21.05.91), figure 1, abstract --	1-14
A	WO 9411849 A1 (VATANEN, HARRI, TAPANI), 26 May 1994 (26.05.94), cited in the application --	1-14

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 April 2000	18 -04- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/01036

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5221838 A (JOSE GUTMAN ET AL.), 22 June 1993 (22.06.93), cited in the application	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/FI 99/01036

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0689316 A2	27/12/95	CA 2149067 A	23/12/95
		JP 8032575 A	02/02/96
US 5018196 A	21/05/91	JP 2112794 C	21/11/96
		JP 8027812 B	21/03/96
		JP 62254543 A	06/11/87
		US 4885777 A	05/12/89
		DE 3687934 A	15/04/93
		EP 0214609 A,B	18/03/87
		JP 62056043 A	11/03/87
		JP 2170184 A	29/06/90
WO 9411849 A1	26/05/94	AT 159602 T	15/11/97
		DE 69314804 D,T	12/02/98
		EP 0669031 A,B	30/08/95
		SE 0669031 T3	
		ES 2107689 T	01/12/97
		FI 925135 A	12/05/94
		FI 934995 A	12/05/94
		GR 3025393 T	27/02/98
		NO 951814 A	09/05/95
US 5221838 A	22/06/93	CA 2096730 A,C	25/06/92
		EP 0564469 A	13/10/93
		SE 0564469 T3	
		EP 0940760 A	08/09/99
		JP 6501329 T	10/02/94
		KR 9707003 B	01/05/97
		WO 9211598 A	09/07/92